ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Conduction of Sheltered Information Providing Multiple Coatings around Data and using Audio as Transporter

Mr. Vikas Kamra[1], Parul[2]

Assistant Professor, CSE, JCDM College of Engineering, Sirsa, India [1]

Student, CSE, JCDM College of Engineering, Sirsa, India [2]

Abstract: The exploration work is regarding the learning of cryptographic and steganography techniques and make available the advancement in security with the amalgamation of these procedures by the side of with the hashing techniques such as MD5 hash method has been worn out for offering the secrecy of information over the network. The communication of information necessitates being secured over the network. This paper projected the multiple coatings approach for security of data which comprises the hashing, cryptographic steps and steganography procedures for encryption and hiding of data. For supplementary security, the LSB technique has been regarded with audio file for hiding of encrypted data. The result has been generated with the MATLAB 2010 version.

Keywords: MD5, LSB, Audio, wav.

I. INTRODUCTION

The data and information is obligatory element of any association that should be protected and confidential. From the protection portions, the information should be obtainable when mandatory. In Network circumstances, information can be broadcasting over the network and interloper can assault on the secret data. Steganography is a phenomenon whose work is to conceal a message surrounded by a cover-media in such a way that others cannot differentiate the occurrence of the message. Steganography utilizes the prospect of hiding data and information into digital multimedia files.

Hiding Data in Audio

This phenomenon of data protection will be additional proficient and well organised as compared to the other methods or techniques. There are two perceptions of contemplation before choosing an programming technique for audio. These are the digital arrangement of the audio and the conduction medium of the audio.

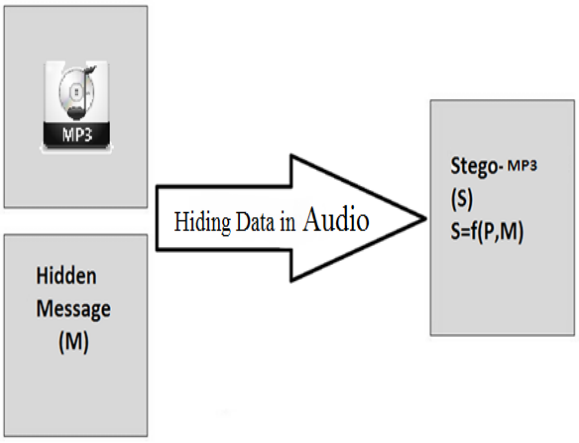


Figure 1 Hiding data in audio

There are three main digital audio formats typically in use

- **Sample Quantization** which is a 16-bit linear sampling structural design used by admired audio layouts.
- **Temporal Sampling Rate** uses chosen frequencies to sample the audio.
- **Perceptual Sampling** This is the third Audio format is Perceptual Sampling.

Least Significant Bit (LSB)

LSB thrashing is a straightforward and speedy scheme for inserting information in an audio signal. It comprises of implanting each and every bit of message in LSB. LSB hiding phenomenon gives a very elevated control competence for conduction of many sorts of data and is easy to put into practice. Also LSB is very easy to combine with other hiding techniques. The LSB procedure takes plus point of the HAS which cannot have the sense of hearing the slight dissimilarity of audio frequencies at the elevated frequency side of the audible spectrum. The LSB system agree to high implanting rate devoid of demeaning the superiority of the audio file. In our research work we are going to use the LSB of data when we use hash of the data. We take LSB of the generated hash value.

Waveform Audio File Format (WAV)

Waveform Audio File Format (WAV) file layout was cooperatively urbanized by IBM and Microsoft companies. WAV was made to store and accumulate sound in files. It is a split part of of Microsoft's Resource Interchange File Format (RIFF) bit stream arrangement for accumulating data in chunks and sub chunks. A WAV file can enclose both compacted/compressed and uncompacted audio but the most widespread WAV audio design is uncompressed audio in the linear pulse code modulation (LPCM) format.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Multiple coatings around data for security

In the multiple layer security scenarios. The LSB of carrier standard is unswervingly introduced with the message bit. So LSB of the transporter medium surrounded the surreptitious Information which is to be concealed. The result of the encoding process is a set of data frames. In this three layer coating the encryption is done on the data also the hash is generated and after all the coatings the data is hide in the audio format so that the attacker will not be able to find the data and will not be able to attack the information.

II. LITERATURE REVIEW

Balgurgi, P.P., Jagtap, S.K., proposed that Security has its importance and application in wide area. It is a measure of human negligence, in desire to seize the latest technological inventions. This measure may have adverse effect on human perception to the deployment of application, which needs serious concern in terms of security. Audio steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. The main challenge in audio steganography is to obtain robust high capacity steganographic systems. The author provides implementation of two level encryption of user data by combining two areas of network security, cryptography and steganography. The combination of LSB technique with XORing method is described in this paper, which gives additional level of security. Varieties of techniques for embedding information in digital audio have been established. They attend the general principles of hiding secret information using audio technology, and an overview of functions and techniques. [1]

Qilin Qi provide Digital steganography is a method used for hiding information in digital images. It can be used for secure communication. There have been many robust digital steganography methods invented in recent decades. The steganographic message can be inserted in multimedia cover signal such as audio, image and video. However, this technique also may be used by malicious users to transmit dangerous information through the Internet beyond the control of security agenciesExisting steganalysis methods or steganography attacking methods which are mostly passive methods cannot be used for analyzing a large volume of digital images in a short time. In addition those passive methods also cannot be generic enough to defeat various steganographic algorithms on the Internet. In this paper, we propose an active attacking model to defeat the rising threat of steganography.

The active protection mechanism is proved to be more effective to protect the integrity of the multimedia data. Based on the active attacking model, a steganography attacking method which is not limited by the types of the steganography methods is proposed. The proposed method can process the digital multimedia data to remove the potential dangerous hidden information while keeping the digital data in a high visual quality. This attack method is based on a proposed transform called Discrete Spring Transform. Some implementations of the Discrete Spring Transform in audio, image and video signals are proposed. The proposed transform causes that the numerical values of the image to be changed dramatically and then the hidden information is not able to be recovered, while at the same time the visual image quality can be maintained. This method is a generic approach for multimedia signals and contains theoretical advantages over similar methods. Our experimental results have demonstrated that the quality of the multimedia signal can be guaranteed while the stego-data are considerably destroyed. [12]

Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade Provide a method to improve the data hiding in all types of multimedia data formats such as image and audio and to make hidden message imperceptible, a novel method for steganography is introduced in this paper. It is based on Least Significant Bit (LSB) manipulation and inclusion of redundant noise as secret key in the message. This method is applied to data hiding in images. For data hiding in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) both are used. All the results displayed prove to be time-efficient and effective. Also the algorithm is tested for various numbers of bits. For those values of bits, Mean Square Error (MSE) and Peak-Signal-to-Noise-Ratio (PSNR) are calculated and plotted. Experimental results show that the stego-image is visually indistinguishable from the original cover-image when n<=4, because of better PSNR which is achieved by this technique. The final results obtained after steganography process does not reveal presence of any hidden message, thus qualifying the criteria of imperceptible message. [3]

Kamalpreet Kaur, DeepankarVerma states that Internet world is characterized by many users among which are crackers and thieves. Hence, the need for a secured system to safely exchange confidential information among users across the web is required. Of such tool is steganography that simply hides the user information under other kind of information such as audio so that no one suspects that a sensitive data is being transferred. Its purpose is to hide the presence of communication. Here three different steganographic methods have been used instead of using one steganographic method. This has been done with a layering approach. This method is named as multi-level steganography. It uses at least two steganographic methods in which one method serves as a carrier for the second one. Multi-Level Steganography has advantage of difficult decoding and sending two or more secret message through a single cover object.

This paper defines a method for audio steganography using LSB coding, parity coding and phase coding technique in multi-level steganography. In this thesis the review of three layered approach for audio multi-level steganography has been presented. Here three secret messages rather than one can be transmitted with a single cover file. In this paper, three permutations of audio steganography methods are compared. The result of the

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

stego audios is compared by PSNR graph. Each permutation has three levels. Three levels of audio steganography can be identified as layer 1, layer 2 and layer 3. This method has provided an effective way to achieve higher security, increased undetectability and the maintained consistency in the clarity of digital audio signal. [4]

Kamal Pradhan, Chinmaya Bhoi presents that the communication system is prone to the interception and improper manipulation by eavesdropper. Audio Steganography is the procedure of hiding the existence of secret information by zipping it into another medium such as audio file. This paper explores the innovative audio Steganography technique in a practical way in order to conceal the preferred information. The proposed system uses LSB (least significant bit) technique for embedding text into an audio file. The text is encrypted using AES (Advanced encryption standard) encryption function and md5 hash function which is used for verifying data integrity of the audio file. The performance of this system is evaluated through a more secure process based on robustness, security and data hiding capacity.[15]

Chintan R. Nagrecha proposes more efficient methods which ensure secure data transfer. One of the method is the audio Steganography. One of the most important and widely used approach of audio steganography is LSB (List significant approach). In this paper we deals with the approach of embedding the bits at higher random layer which leads towards difficult discovery of data. Main aim of this paper is to improve capacity and robustness of this approach. The combination of well known compressive algorithms and given embedding approach gives observable result. This leads to improve the capacity of host audio and robustness. [10]

III. OBJECTIVES

The main objective is to make available three layer coating around the data for security purpose. The three layers will sheltered the content from intruders. This practice will protect the secret contented over the network. To make the data more protected and secretive the three coatings would b provided.

So the main objectives are:

- Sentinel the content from intruder
- Secure the private information
- Audio format must not be altered after the encryption process
- To obscure messages contained by other innocuous messages in a way that does not agree for any adversary to even perceive that there is an accomplishing message in attendance.
- Make the data additional sheltered and confidential.

Problem Statement

Steganography is now being extensive area to study. As the requirement of protected and sheltered intercommunication further enhanced to a great extent. From the few decades lot of dissimilar methods of hiding and providing coatings around the information has grown up. Some of the existing phenomenon's for covering data are used in great extent.

These phenomenon include LSB technique for hiding the data, generating the hash functions, encryption can be done by using the DES i.e. data encryption standard. LSB is the most trendy Steganography technique. It bury the underground message in the media file based on it its double coding. It uses the LSB algorithm. In two layer security, the data is not a great deal protected In network scenario, safely transmission of data is main characteristic it is decisive because information and data can be discovered.

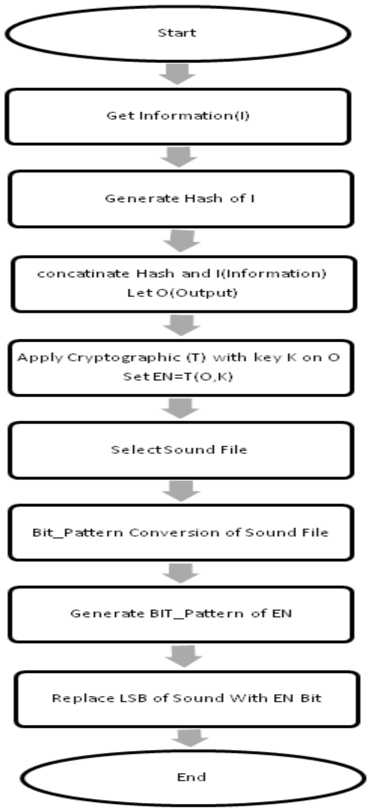
IV. PROPOSED METHODOLOGY

In this algorithm is proposed for the security to data. Algorithm is used for solving the problem step by step which can be implemented with help of programming in any language. In the three layer security scenario, the different approach will be used on every layer. The algorithm below explains the flow of security mechanism applied on sound file bit stream and hashed-Encrypted information for keep the information hide.

1. Start
2. Get Confidential Information(I)
3. Let Hash Output S
4. Initialize Hash Algorithm-Denoted H
5. Generate Hash of I
6. For each Character(C_i) in I
   $\sum_{i=0}^{length(I)} S = H(Ci)$
7. If(Hash Successful) then
8. Let Output O
9. Concatenate Hash(S) and I(Confidential Information)
   Set O =concatenate(S,I)//First Layer Completed
10. Cryptographic technique selection, Let Technique (T) and Key (K)
11. Let EN (Encrypted Information)
12. Set EN=Encrypt T(O from Step 9,K)//Second Layer Completed
13. Select Sound File (Let name is SO)
14. Repeat below Steps until Low-Bit Encoding Complete
15. Convert SO in Bit Pattern
16. Initialize of EN Bit Conversion
17. Let BS(Bit Sequence)
18. Set C Character in EN
19. For Each(C in EN)
    $\sum_{i=0}^{length(EN)} BS = Bit(Ci)$
20. If BS Completed Successfully then
21. Replace LSB (Step: 15) with BS Bytes//Third Layer Completed.
22. Else Move to Step 19.
23. Stop

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015



Flow chart 1 proposed algorithm

V. RESULTS AND ANALYSIS

In first step, the hash has been generated of input text. The input text is Parul1. The hash will be generated and concatenated.

```
>> msg='Parul1';
%22 length max
hash = DataHash(msg);
subHash=hash(1:2); % add hash of length 2.
msg=strcat(msg,subHash);
%process 1st 8 bytes
msg1=msg(1:8);
str = reshape(dec2bin(double(msg1),8).',[],64)
input64 = str;
mode = 'ENC';
key = [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[output64] = DES(input64,mode,key);

str =

0101000001100001011100100111010101101100001100010011001001100110
```

Figure 2 Hash generation and concatenation

The concatenated result is Parul12f. This layer1 has been completed. In the second layer, this information will be as input to the cryptographic technique which will generate the encrypted information. The information will be converted to binary and then, encrypts by the key. The resulted output will gives the sequence of bits.
0110111001101001011100110110100001110101001100010110001000110000

At this stage, the number of bits will be hidden in the audio wav file by LSB Technique by replacing the LSB of wav file with the resulted bits and HAS (Human Auditory System) will not be able to detect the wav file. The wav file before hide and after hide should remain same along with the properties of the wav. This can be visualized by comparing the waveforms of original and modified wav file.

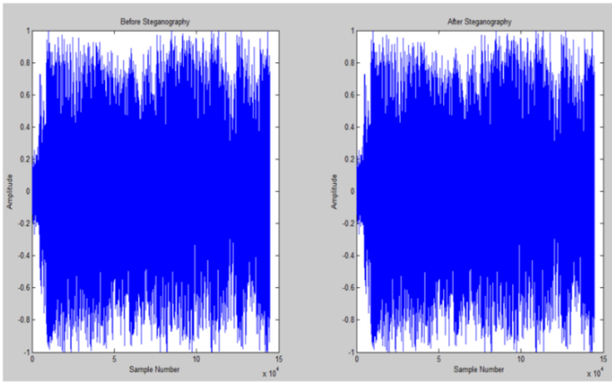


Figure 3 Original and Modified Wave

VI. CONCLUSION AND FUTURE WORK

The key idea of our projected algorithm is to avoid entrenching in a hushed periods of congregation audio indication due to compassion of Human Auditory System (HAS) so it will have an effect on the perceptual intelligibility deformation in a certain manner. Hash produce is functional for confirm the discretion of information. The planned work will calculate the hash and then reconstruct the message by means of hash and then apply the cryptography algorithm to encrypt the complete data, then LSB procedure will put out of sight the information in audio file. The experimental results illustrate the accurateness of system and will be advantageous for organization. Also far above the ground perceptual simplicity is achieved by LSB of host audio signal which are worn for data hiding and method has advanced the capability and forcefulness of data concealed in the audio file.

In future, the complexity of the Sound file can be enhanced by some method and practices for put out of sight the upper limit of data in audio files. SNR (Signal to Noise ratio) factor can be regarded as to calculate the presentation of schemes. The procedures should be practicable in such as way that the HAS (Human Auditory System) will not be able to perceive the unseen information

REFERENCES

[1] Balgurgi, P.P., Jagtap, S.K., "Intelligent processing: An approach of audio steganography", Communication, Information & Computing Technology (ICCICT), 2012
[2]Gopalan, K., Qidong Shi "Audio Steganography Using Bit Modification - A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", Computer communications and Networks (ICCCN), 2010

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

[3] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade" An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution ", International Journal of Computer Applications, 2013

[4]] Kamalpreet Kaur, DeepankarVerma" Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", International Journal of Advanced Research in Computer Science and Software Engineering, 2014

[5] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi" Overview: Main Fundamentals for Steganography", 2010

[6] Usha, S. "A secure triple level encryption method using cryptography and steganography", Computer Science and Network Technology (ICCSNT), 2011

[7] Djebbar, F.; Ayad, B. ; Hamam, H. ; Abed-Meraim, K "A view on latest audio steganography techniques", Innovations in Information Technology (IIT), 2011

[8] Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan "New Design for Information Hiding with in Steganography Using Distortion Techniques", 2010

[9] Asad, M., Gilan, J., "Khalid, A, "An enhanced least significant bit modification technique for audio steganography", Computer Networks and Information Technology (ICCNIT), 2011

[10] Chintan R. Nagrecha, Prof. Prashant B. Swadas" Audio Steganography with Various Compression Algorithms to Improve Robustness and Capacity ",International Journal of Advanced Research in Computer Science and Software Engineering, 2014

[11] Arvind Kumar, Km. Pooja "Steganography- A Data Hiding Technique," 2010

[12] Qilin Qi" A study on countermeasures against steganography: An active warden approach", 2013

[13] Sujay Narayana and Gaurav Prasad" Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions", 2010

[14] Nugraha, R.M. "Implementation of Direct Sequence Spread Spectrum steganography on audio data", Electrical Engineering and Informatics (ICEEI), 2011

[15] Kamal Pradhan, Chinmaya Bhoi" Robust Audio Steganography Technique using AES algorithm and MD5 hash", International Journal of Innovative Research in Advanced Engineering (IJIRAE), 2014

[16] Shahadi, H.I., Jidin, R., "High capacity and inaudibility audio steganography scheme Information Assurance and Security (IAS)", 2011